AMENDMENT TO THE CLAIMS

1. (original): A method for providing access to secure data through a portable computing system during a specified time, wherein said method comprises:

establishing a connection between said portable computing system and a base computing system to provide for transfer of data between said portable computing system and said base computing system;

verifying identity of said base computing system within said portable computing system;

resetting a timer within said portable computing system to run for a specified time; and

providing access to said secure data only when said timer is running.

2. (original): The method of claim 1, wherein said step or verifying identity of said base computing system comprises:

receiving and storing a public cryptographic key from said base computing system during an initialization process,

following said initialization process, generating a random number within said portable computing system;

transmitting said random number to said base computing system;

receiving a number transmitted from said base computing system;

decrypting said number transmitted from said base computing system to form a decrypted number; and

determining that said decrypted number matches said random number.

3. (original): The method of claim 1, additionally comprising a step of verifying whether a password is entered correctly in said portable computing system.

4. (original): The method of claim 3, wherein said step of verifying whether a password is entered correctly includes:,

transmitting an initial password to said base computing system during an initialization process,

storing said initial password within said base computing system;

following said initialization process, transmitting a present password to said base computing system;

determining in said base computing system that said initial password matches said present password;

transmitting an approval code from said base computing system to said portable computing system; and

determining that. said approval code has been received.

5. (original): The method of claim 1, wherein said connection is established through a switched telephone network. '

6. (original): The method of claim 1, wherein

said timer includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

7. (currently amended): A method providing for access to secure data through a portable computing system, wherein said access to said secure data is limited to a specified time, and wherein said method comprises:

initializing a base computing system and said portable computing system to work together as a system by an initialization process comprising:

storing data identifying said base computing system within said portable computing system; and

resetting said portable computing system by a reset process following said initialization process including:

establishing a connection to transmit data between said portable computing system and a base computing system;

determining, using said data identifying said base computing system, that said connection has been made between said portable computing system and said base computing system;

setting a timer within said portable computing system to run until said specified time has expired;

determining if said timer is running; and

providing access to said secure data only when said timer is running.

8. (original): The method of claim 7, wherein

said initialization process additionally includes determining whether said data identifying abase computing system has been previously stored in said portable computing system;

if said data identifying a base computing system is determined to have been previously stored, said data identifying a base computing system remains without being overwritten during said initialization process.

9. (original): The method of claim 8, wherein said data identifying said base computing is a public cryptographic key of said base computing system, and wherein said process of determining that said connection has been made between said portable computing system and said base computing system includes:

generating and storing random number within said portable computing system;

transmitting said random number from said portable computing system to said base computing system;

encrypting said random number within said base computing system with a private cryptographic key of said base computing system to form an encrypted number;

transmitting said encrypted number from said base computing system to said portable computing system;

decrypting said encrypted number within said portable computing system with said public cryptographic key of said base computing system to form a decrypted number; and

comparing said decrypted number with said random number stored within said portable computing system.

10. (original): The method of claim 8, wherein

said timer includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

11, (original): The method of claim 8, wherein

said method additionally comprises receiving an input corresponding to a time, and

setting said specified time according to said input.

12. (original): The method of claim 8, additionally comprising storing a cryptographic public cryptographic key of said portable computing system within said base computer system.

13. (currently amended): The method of claim 8, wherein

said initialization process additionally includes receiving a present password as an input, determining if a password has been previously stored, and storing said present password in response to a determination that said password has not been previously stored, ~~arid~~

said reset process additionally includes receiving a present password as an input and determining if said present password matches a stored password; and

said timer is set within said portable computing system only in response to a determination that said present password matches said stored password.

14. (original): The method of claim 13, wherein

said present password is received as an input within said portable computing system,

said present password is transmitted from said portable computing system to said base computing system,

said present password is stored within said base computing system following a determination that a password is not previously stored within said base computing system;

a determination is made in said base computing system of whether said present password matches a stored password,

said reset process additionally includes transmitting an approval code from said base computing system to said portable computing system in response to a determination that said present password matches said stored password, and

said timer is set within said portable computing system in response to receiving said approval code.

15. (original): The method of claim 14, wherein said data identifying said base computing is a public cryptographic key of said base computing system, and wherein said process of determining that said connection has been made between said portable computing system and said base computing system includes:

generating and storing random number within said portable computing system;

concatenating said random number and said present password within said portable computing system to form a concatenated number;

encrypting said concatenated number within said portable computing system with said public cryptographic key of said base computing system to form a first encrypted number;

transmitting said first encrypted number from said portable computing system to said base computing system

decrypting said first encrypted number within said base computing system with a private cryptographic key of said base computing system to form a decrypted number;

dividing said decrypted number to form a decrypted random number and said present password;

encrypting said decrypted random number within said base computing system with a private cryptographic key of said base computing system to form a second encrypted number;

transmitting said second encrypted number from said base computing system to said portable computing system;

decrypting said second encrypted number within said portable computing system with said public cryptographic key of said base computing system to form a decrypted number; and

comparing said decrypted number with said random number stored within said portable computing system.

16. (original): A system for providing controlled access to secure data, wherein said system comprises:

a portable computing system providing said controlled access to secure data during a specified time, wherein said portable computing system includes first processing means, first storage means, and a timer;

a base computing system including second processing means and second storage means;

a connection between said portable computing system and said base computing system for transmitting data between said portable computing system and said base computing system; and

a first program, executing within said first processing means, causing said portable computing system to perform a process including:

determining if a public cryptographic key is stored in a first location within said first storage means;

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code, receiving said public cryptographic key, and storing said public cryptographic key in said first location;

transmitting a first code;

receiving a response to said first code;

determining from said response to said first code if a connection has been made to said base computing system; and

setting said timer to run until said specified time has expired;

a subroutine executing within said first processing means, causing said portable computing system to perform a process including:

determining if said timer is running; and

providing access to said secure data only when said timer is running; and

a second program, executing within said second processing means, causing said base computing system to perform a process including:

receiving said request code;

in response to receiving said request code, transmitting a public cryptographic key of said base computing system to said portable computing system;

receiving said first code; and

in response to receiving said first code, transmitting said response to said first code.

17. (original): The system of claim 16, wherein

said first storage means includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

18. (original): The system of claim 17, wherein

said step of transmitting a first code includes generating a random number, storing said random number in a second location within said first storage, and transmitting said random number to said base computing system as said first code,

said step of transmitting said response to said first code includes encrypting

said random number with a private cryptographic key of said base computing system to form an encrypted random number, and transmitting said encrypted random number as said response to said portable computing system as said

response to said first code, and

said step of determining from said response to said first code if a connection has been made to said base computing system includes decrypting said encrypted number to form a decrypted number and comparing said decrypted number with said random number stored in said second location within said first storage.

19. (original): The system of claim 18, wherein

said first processing means includes a first microprocessor and a first cryptographic processor,

said encrypted number is decrypted in said first cryptographic processor,

said first storage means includes first secure storage accessed only through

said first cryptographic processor, and

said first location and said timer register within said first storage means are within said secure storage.

20. (original): The system of claim 18, wherein

said second processing means includes a second microprocessor and a second cryptographic processor,

said random number is encrypted to form said encrypted number within said second cryptographic processor,

said second storage means includes second secure storage accessed only through said second cryptographic processor, and

said private cryptographic key of said base computing system is stored within said second secure storage.

21. (original): The system of claim 16, wherein

said portable computing system additionally includes a display,

said first program additionally causes a successful completion message to

be displayed on said display in response to a determination from said response to said first code that a connection has been made to said base computing system,

and said first program additionally causes an error message to be displayed on said display in response to a determination from said response to said first code that a connection has not been made to said base computing system.

22. (original): The system of claim 16, wherein

said portable computing system additionally includes a display and a keyboard, and

said first program causes said portable computing to perform a process additionally including displaying a menu, receiving a user input from said keyboard as said menu is displayed, and determining said specified time from said user input.

23. (currently amended): The system of claim 16, wherein

said portable computing system additionally includes a display and a keyboard,

said first program causes said portable computing to perform a process additionally including displaying a menu and receiving a password from said keyboard as said menu is displayed,

said step of transmitting a first code includes:

generating a random number;

storing said random number in a second location within said first storage;

concatenating said random number with said password to form a concatenated number

encrypting said concatenated number with a private cryptographic key of said portable computer system stored in a third location within said first storage means to form said first code; and

transmitting said random number to said base computing system as said first code,

said step of transmitting said response to said first code includes:

decrypting said first code with a private cryptographic key of said base computing system stored in a fourth location within said second storage means;

separating said password from said random number;

determining whether said password separated from said random number matches a password stored;

encrypting said random number with a private cryptographic key of said base computing system to form an encrypted random number, and

~~determining if and~~ in response to determining that said password separated from said random number matches said password stored, transmitting said encrypted random number as said response to said portable computing system as said response to said first code,

said second program causes said base computing system to perform a process additionally including:

determining if a password is stored in a fifth location within said second storage means;

in response to a determination that a password is not stored in said fifth location, storing said password separated from said random number in said fifth location;

in response to a determination that a password is stored in said fifth location, comparing said password stored in said fifth location with said password separated from said random number;

in response to determining that said password stored in said fifth location matches said password separated from said random number, encrypting said random number and to form a transmitting an approval code to said portable computing system as said response to said first code; and

said step of determining from said response to said first code if a connection has been made to said base computing system includes determining that said approval code has been received.

24. (original): The system of claim 23, wherein

said second program causes said base computing system to perform a process additionally including, in response to determining that said password stored in said fifth location does not match said password separated from said random number, transmitting an error code to said portable computing system as said response to said first code

said first program causes said portable computing to perform a process additionally including displaying a successful completion message on said display in response to receiving said approval code, and displaying an error message on said display in response to receiving said error code.

25. (original): The system of claim 23, wherein

said first storage means includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

26. (original): The system of claim 23, wherein

said first processing means includes a first microprocessor and a first cryptographic processor,

said concatenated number is encrypted in said first cryptographic processor,

said first storage means includes first secure storage accessed only through said first cryptographic processor, and

said secure storage includes said first location, said third location, and said timer register within said first storage means.

27. (original): The system of claim 23, wherein

said second processing means includes a second microprocessor and a second cryptographic processor,

said random number is encrypted to form said encrypted number within said second cryptographic processor,

said second storage means includes second secure storage accessed only through said second cryptographic processor, and

said fourth and fifth locations within said second storage means are within said second secure storage.

28. (original): The system of claim 23, wherein

said step of transmitting a request code includes transmitting a public cryptographic key of said portable computing system, and

said step of receiving a request code includes storing said public cryptographic key of said portable computing system in a sixth location within said second storage means.

29. (original): A computer readable medium within a portable computing system, wherein said computer readable medium has computer readable instructions for performing a method comprising:

determining if a public cryptographic key is stored in a first location within said first storage means;

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code, receiving said public cryptographic key, and storing said public cryptographic key in said first location;

transmitting a first code;

receiving a response to said first code;

determining from said response to said first code if a connection has been made to a base computing system; and

setting a timer to run until a specified time has expired.

30. (original): The computer readable medium of claim 29, wherein said step of setting aid timer includes storing a number corresponding to said specified time in a timer register.

31. (original): The computer readable medium of claim 29, wherein

said step of transmitting a first code includes generating and storing a random number, and transmitting said random number to said base computing system as said first code, and

said step of determining from said response to said first code if a connection has been made to a base computing system includes decrypting an encrypted number to form a decrypted number and comparing said decrypted number with said random 'number.

32. (original): The computer readable medium of claim 29, wherein said method additionally comprises:

displaying a successful completion message in response to receiving an approval code; and

displaying an error message in response to receiving an error code.

33. (original): The computer readable medium of claim 29, wherein said method additionally comprises:

displaying a menu;

receiving an input from a keyboard as said menu is displayed; and

determining said specified time from said input.

34. (original): The computer readable medium of claim 29, wherein

said method additionally includes displaying a menu and receiving a password from a keyboard as said menu is displayed,

said step of transmitting a first code includes:

generating a random number;

storing said random number in a second location within said first storage;

concatenating said random number with said password to form a concatenated number,

encrypting said concatenated number with a private cryptographic key of said portable computer system stored in a third location within said first storage means to form said first code; and

transmitting said random number to said base computing system as said first code.

35. (original): In a portable computing system having a user interface including a display and a keyboard, a method for limiting access to secure data to a specified time, wherein said method comprises:

displaying a screen location for entering a number;

accepting an input from said keyboard;

displaying said input from said keyboard in said screen location;

calculating a number determining said specified time as a function of said input from said keyboard;

generating a random number;

transmitting said random number to a base computing system;

receiving an encrypted number from said base computing system,

decrypting said encrypted number with a public cryptographic key stored within said portable computing system to form a decrypted number;

determining if said random number matches said decrypted number; and

in response to determining that said random number matches said decrypted number, setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said time is running.

36. (original): The method of claim 35, additionally comprising:

displaying a successful completion message in response to determining that said random number matches said decrypted number; and

displaying an error message in response to determining that said random number does not match said decrypted number.

37. (currently amended): In a portable computing system having a user interface including a display
and a keyboard, a method for limiting access to secure data to a specified time, wherein said method comprises:

displaying a first screen location for entering a password and a second screen location for entering a number;

accepting a first input from said keyboard;

generating a password from said first input;

accepting a second input from said keyboard;

displaying said input from said keyboard in said second screen location;

calculating a number determining said specified time as a function of said second input from said keyboard;

generating a random number;

encrypting said password with a public cryptographic key stored in said portable computing system;

transmitting said random number to a base computing system;

receiving an encrypted number from said base computing system,

decrypting said encrypted number with said public cryptographic key stored within said portable computing system to form a decrypted number;

determining if said random number matches said decrypted number; and

in response to determining that said random number matches said decrypted number, setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said ~~time~~ timer is running.

38. (original): The method of claim 35, additionally comprising:

displaying a successful completion message in response to determining that said random number matches said decrypted number; and

displaying an error message in response to determining that said random number does not match said decrypted number and in response to receiving an error code from said base system.

39 (new): The method of claim 1, wherein said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

40 (new): The method of claim 7, wherein said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

41. (new): The system of claim 16, wherein said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

42. (new): The portable computing system of claim 35, wherein, within said method, said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

43. (new): The portable computing system of claim 37, wherein, within said method, said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.